



TITLE:

Key Assertions and Backward Substitutions (アルゴリズムにおける証明論)

AUTHOR(S):

TAKASU, SATORU

CITATION:

TAKASU, SATORU. Key Assertions and Backward Substitutions (アルゴリズムにおける証明論). 数理解析研究所講究録 1975, 236: 190-196

ISSUE DATE:

1975-05

URL:

<http://hdl.handle.net/2433/105498>

RIGHT:

KEY ASSERTIONS AND BACKWARD SUBSTITUTIONS. S.TAKASU (RIMS)

Definition: Let T be a mathematical theory and M a model of T . We assume that a correspondence between $m \in M$ and a term \bar{m} in T is given (for example natural number m and numeral $\bar{m} = 0^{(m)}$ where $0^{(m)}$ is the result of m fold applications of successor function to 0). A function $f(x_1, \dots, x_n)$ defined within M is said to be representable^[8.1] in T if there exists a well-formed formula $\Gamma(x_1, \dots, x_n, x_{n+1})$ with $n+1$ free variables such that for any $(m_1, \dots, m_n) \in M^n$,

- (1) if $m_{n+1} = f(m_1, \dots, m_n)$ then $\vdash_T \Gamma(\bar{m}_1, \dots, \bar{m}_{n+1})$, and
- (2) $\vdash_T (\exists! x_{n+1}) \Gamma(x_1, \dots, x_{n+1})$.

Example . We consider the flowchart of Fig.2.3 which computes $\text{gcd}(m, n)$. To this flowchart we attach the formulas:

$$\varphi(m, n) \equiv m > 0 \wedge n > 0,$$

$$p(m, n, c, d, r) \equiv c = m \wedge d = n \wedge \varphi(m, n)$$

$$\psi(m, n, d) \equiv d = \text{gcd}(m, n)$$

and the predicate $q(m, n, c, d, r)$ is to be determined. ($s(m, n, c, d, r)$ will be used when we consider EB_P .) We further parametrize the predicates p and q to the predicates P and Q respectively, introducing a control variable i which expresses the number of visits to the loop.

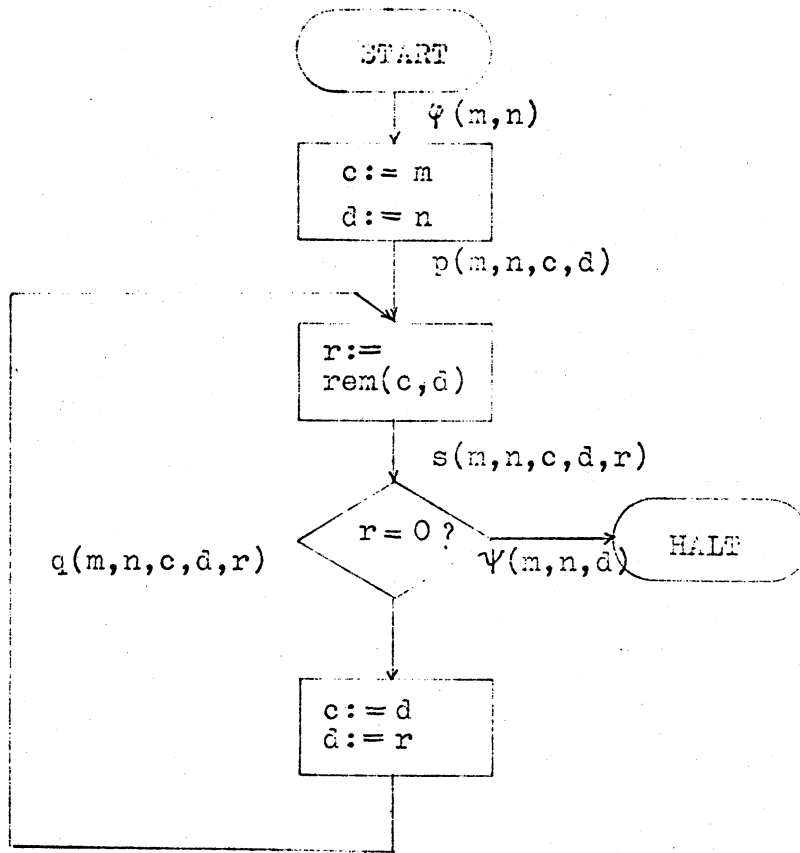


Fig.2.3. A flowchart to compute $\gcd(m, n)$

We have the system EF_P as follows:

$$Q(x, y, 0) \equiv c = m \wedge d = n \wedge i = 0 \wedge \varphi(m, n) \quad ,$$

$$Q(x, y, \bar{i}) \equiv \exists c' \exists d' \exists r'. Q(x, c', d', r', \overline{i-1}) \wedge r = \text{rem}(c, d)$$

$$\wedge c = d' \wedge d = r \quad ,$$

$$(\exists r'. Q(m, n, c, d, r', \bar{i}) \wedge r = \text{rem}(c, d) \wedge r = 0) \supset d = \gcd(m, n)$$

where $x = (m, n)$ and $y = (c, d, r)$. For each numeral \bar{i} , we rewrite

EF_P as follows:

$$Q(m, n, c^{(i)}, d^{(i)}, r^{(i)}, \bar{i})$$

$$\equiv \exists c^{(i-1)} \exists d^{(i-1)} \exists r^{(i-1)}. Q(m, n, c^{(i-1)}, d^{(i-1)}, r^{(i-1)}, \overline{i-1})$$

$$\wedge r^{(i)} = \text{rem}(c^{(i-1)}, d^{(i-1)}) \wedge r^{(i)} \neq 0$$

$$\wedge c^{(i)} = d^{(i-1)} \wedge d^{(i)} = r^{(i)},$$

.....

$$\begin{aligned}
Q(m, n, c^{(1)}, d^{(1)}, r^{(1)}, 1) \\
\equiv \exists c^{(0)} \exists d^{(0)} . c^{(0)} = m \wedge d^{(0)} = n \wedge m > 0 \wedge n > 0 \\
\wedge r^{(1)} = \text{rem}(c^{(0)}, d^{(0)}) \wedge r^{(1)} \neq 0 \\
\wedge c^{(1)} = d^{(0)} \wedge d^{(1)} = r^{(1)}.
\end{aligned}$$

If we set

$$\begin{aligned}
a^{(0)} &= 0, \\
b^{(0)} &= 1, \\
\underline{a}^{(0)} &= 1, \\
\underline{b}^{(0)} &= 0,
\end{aligned}$$

and

$$\begin{aligned}
a^{(i)} &= \underline{a}^{(i-1)} - \text{quo}(c^{(i-1)}, d^{(i-1)}) \times a^{(i-1)}, \\
b^{(i)} &= \underline{b}^{(i-1)} - \text{quo}(c^{(i-1)}, d^{(i-1)}) \times b^{(i-1)}, \\
\underline{a}^{(i)} &= \underline{a}^{(i-1)}, \\
\underline{b}^{(i)} &= \underline{b}^{(i-1)},
\end{aligned}$$

then there hold

$$\begin{aligned}
c^{(j)} &= \underline{a}^{(j)} m + \underline{b}^{(j)} n, \text{ and} \\
d^{(j)} &= a^{(j)} m + b^{(j)} n, \text{ where } j = 0, 1, 2, \dots
\end{aligned}$$

Since $a^{(j)}$, $b^{(j)}$, $\underline{a}^{(j)}$ and $\underline{b}^{(j)}$ are recursively defined functions of m , n , and j , they are representable in the elementary number theory so that we have

$$\begin{aligned}
Q(m, n, c, d, r, i) &\equiv c = \underline{a}^{(i)} m + \underline{b}^{(i)} n \wedge d = a^{(i)} m + b^{(i)} n \\
&\wedge r = d \wedge r \neq 0 \wedge m > 0 \wedge n > 0
\end{aligned}$$

where i is a proper variable of the predicate Q . Therefore we have

$$\begin{aligned}
q(m, n, c, d, r) &\equiv \bigvee_{i=1}^{\infty} Q(m, n, c, d, r, i) \\
&\equiv \exists i . i \geq 1 \wedge Q(m, n, c, d, r, i).
\end{aligned}$$

Now it is clear that the implication formula of $\text{EF}_P(c)$ or $\text{EF}_P(Q)$ holds if one knows the theorem

$$\begin{aligned}
\exists a \exists b \exists \underline{a} \exists \underline{b} . c = \underline{a}m + \underline{b}n \wedge d = am + bn \wedge r = 0 \\
\supset d = \text{gcd}(m, n).
\end{aligned}$$

We consider the system EB_p for the flowchart of Fig.2.3 where we use $s(m,n,c,d,r)$ instead of $a(m,n,c,d,r)$:

$$\begin{aligned} p(m,n,c,d,r) &\supset s(m,n,c,d,\text{rem}(c,d)), \\ s(m,n,c,d,r) \wedge r \neq 0 &\equiv s(m,n,c,d,\text{rem}(c,d)), \\ s(m,n,c,d,r) \wedge r = 0 &\equiv \psi(m,n,d). \end{aligned}$$

First we have the followings by the process of substitution:

$$\begin{aligned} s(m,n,c,d,r) &\equiv s(m,n,c,d,r) \wedge r = 0 \vee s(m,n,c,d,r) \wedge r \neq 0, \\ &\equiv \psi(m,n,d) \wedge r = 0 \vee s(m,n,f(c,d,r),g(c,d,r),h(c,d,r)), \\ &\dots\dots\dots \\ &\equiv \bigvee_{i=0}^k \left\{ \psi(m,n,f^{(i)}(c,d,r)) \wedge h^{(i)}(c,d,r) = 0 \right. \\ &\quad \left. \wedge \left(\bigwedge_{j=0}^{i-1} h^{(j)}(c,d,r) \neq 0 \right) \right\} \\ &\quad \vee \left\{ s(m,n,f^{(k+1)}(c,d,r),g^{(k+1)}(c,d,r),h^{(k+1)}(c,d,r)) \right. \\ &\quad \left. \wedge \left(\bigwedge_{j=0}^k h^{(j)}(c,d,r) \neq 0 \right) \right\} \dots\dots (*) \end{aligned}$$

where $f^{(i)}$, $g^{(i)}$ and $h^{(i)}$ are defined by setting

$$f(c,d,r) = d, \quad g(c,d,r) = r, \quad h(c,d,r) = \text{rem}(d,r),$$

and

$$\begin{aligned} f^{(0)}(c,d,r) &= c, \quad g^{(0)}(c,d,r) = d, \quad h^{(0)}(c,d,r) = r, \\ f^{(i)}(c,d,r) &= f(f^{(i-1)}(c,d,r),g^{(i-1)}(c,d,r),h^{(i-1)}(c,d,r)), \\ g^{(i)}(c,d,r) &= g(f^{(i-1)}(c,d,r),g^{(i-1)}(c,d,r),h^{(i-1)}(c,d,r)), \\ h^{(i)}(c,d,r) &= h(f^{(i-1)}(c,d,r),g^{(i-1)}(c,d,r),h^{(i-1)}(c,d,r)). \end{aligned}$$

If we make explicit the operations, then the previously defined functions $a^{(j)}$, $b^{(j)}$, $\underline{a}^{(j)}$ and $\underline{b}^{(j)}$ where their arguments are c and d this time instead of m and n respectively, define the above functions, namely we have

$$\begin{aligned}
f^{(j)}(c,d,r) &= \underline{a}^{(j)} c + \underline{b}^{(j)} d, \\
g^{(j)}(c,d,r) &= a^{(j)} c + b^{(j)} d, \\
h^{(j)}(c,d,r) &= a^{(j+1)} c + b^{(j+1)} d.
\end{aligned}$$

Therefore the suffix j can be considered as a proper variable of predicates.

Now we set

$$\begin{aligned}
K(m,n,c,d,r) &\equiv \bigvee_{i=0}^{\infty} \left\{ \psi(m,n,g^{(i)}(c,d,r)) \right. \\
&\quad \left. \wedge h^{(i)}(c,d,r)=0 \wedge \left(\bigwedge_{j=0}^{i-1} h^{(j)}(c,d,r) \neq 0 \right) \right\}.
\end{aligned}$$

Then from (*) we have $K(m,n,c,d,r) \supset s(m,n,c,d,r)$. On the other hand

$$\begin{aligned}
g^{(1)} &= \text{rem}(c,d) < g^{(0)} = d, \\
g^{(j+1)} &= \underline{a}^{(j+1)} c + \underline{b}^{(j+1)} d \\
&= (\underline{a}^{(j)} - \text{quo}(f^{(j)}, g^{(j)}) \underline{a}^{(j)}) c \\
&\quad + (\underline{b}^{(j)} - \text{quo}(f^{(j)}, g^{(j)}) \underline{b}^{(j)}) d \\
&= \underline{a}^{(j)} c + \underline{b}^{(j)} d - \text{quo}(f^{(j)}, g^{(j)}) (\underline{a}^{(j)} c + \underline{b}^{(j)} d) \\
&= f^{(j)} - \text{quo}(f^{(j)}, g^{(j)}) g^{(j)} \\
&= \text{rem}(f^{(j)}, g^{(j)}) < g^{(j)},
\end{aligned}$$

namely,

$$d = g^{(0)} > g^{(1)} > \dots > g^{(j)} > \dots \geq 0$$

and therefore

$$s(m,n,c,d,r) \supset \exists j. h^{(j)}(c,d,r) = 0$$

so that there holds

$$s(m,n,c,d,r) \supset K(m,n,c,d,r).$$

Hence we have

$$s(m,n,c,d,r) \equiv K(m,n,c,d,r).$$

Using the properties of gcd we have

$$\begin{aligned}
 & \Psi(m, n, g^{(i)}(c, d, r)) \wedge h^{(i)}(c, d, r) = 0 \\
 & \equiv \gcd(f^{(i)}(c, d, r), g^{(i)}(c, d, r)) = g^{(i)}(c, d, r) \\
 & \quad \wedge g^{(i)}(c, d, r) = \gcd(m, n) \wedge h^{(i)}(c, d, r) = 0 \\
 & \equiv \gcd(c, d) = \gcd(m, n) \wedge g^{(i)}(c, d, r) = \gcd(m, n) \\
 & \quad \wedge h^{(i)}(c, d, r) = 0
 \end{aligned}$$

and

$$\begin{aligned}
 & \bigwedge_{j=0}^{i-1} h^{(j)}(c, d, r) \neq 0 \\
 & \equiv \forall j. j < i \supset h^{(j)}(c, d, r) \neq 0
 \end{aligned}$$

so that we conclude

$$\begin{aligned}
 & s(m, n, c, d, r) \equiv \gcd(m, n) = \gcd(c, d) \\
 & \quad \wedge \exists i. g^{(i)}(c, d, r) = \gcd(m, n) \wedge h^{(i)}(c, d, r) = 0 \\
 & \quad \wedge \forall j. j < i \supset h^{(j)}(c, d, r) \neq 0 .
 \end{aligned}$$

Here we note that the implication formula of EB_P clearly describes the termination of P .

BIBLIOGRAPHY

- [1] Engeler, E. : Algorithmic Properties of Structures,
Math. Systems Theory 1(1967)183-195.
- [2] Engeler, E. : Formal Languages: Automata and Structures,
81pp., Markham, 1968.
- [3] Engeler, E. : Structure and Meanings of Programs,
Symposium on Semantics of Algorithmic Languages,
Springer-Verlag, pp89-101, 1971.
- [4] Floyd, R.W. : Assigning Meanings to Programs, in Proc.
Sym. in Applied Math. 19, Mathematical Aspects
of Computer Sciences (Schwartz, J.T. ed.),
AMS, (1967) pp.19-32.
- [5] Hirose, K. and Oya, M. : General Theory of Flowcharts,
U.S.-Japan Computer Conference Proceedings,
(1972) 367-371.
- [6] Manna, Z. : The Correctness of Programs, J. of Computer and
Systems Sciences, 3(1969)119-127.
- [7] Manna, Z. : Properties of Programs and the First-Order
Predicate Calculus, Jour. ACM, 16(1969)244-255.
- [8] Mendelson, E. : Introduction to Mathematical Logic,
Van Nostrand, 1964.
- [9] Smullyan, R.M. : First-Order Logic, Springer-Verlag, 1968.
- [10] Engeler, E : Algorithmic Approximations,
Jour. of Computer and Systems Sciences
5(1971)67-82,